Security Implications of OPC, OLE, DCOM, and RPC in Control Systems

OPC is a collection of software programming standards and interfaces used in the process control industry. It is intended to provide open connectivity and vendor equipment interoperability. The use of OPC technology simplifies the development of control systems that integrate components from multiple vendors and support multiple control protocols. OPC-compliant products are available from most control system vendors, and are widely used in the process control industry.

OPC was originally known as OLE for Process Control; the first standards for OPC were based on underlying services in the Microsoft Windows computing environment. These underlying services (OLE [Object Linking and Embedding], DCOM [Distributed Component Object Model], and RPC [Remote Procedure Call]) have been the source of many severe security vulnerabilities. It is not feasible to automatically apply vendor patches and service packs to mitigate these vulnerabilities in a control systems environment. Control systems using the original OPC data access technology can thus inherit the vulnerabilities associated with these services.

Current OPC standardization efforts are moving away from the original focus on Microsoft protocols, with a distinct trend toward web-based protocols that are independent of any particular operating system. However, the installed base of OPC equipment consists mainly of legacy implementations of the OLE for Process Control protocols.

Due to the sensitivity of the material, the full text document will only be available to members of the US-CERT secured portal at:

https://us-cert.esportals.net/member/libraryV3/rhsIndex.cfm?action=9&returnAction=32&libid=5435

For additional information on Control Systems, please visit the following site:

www.us-cert.gov/control_systems